Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

(Ag)

Legislative & Regulatory Counsel, NSA

14 Nov 85

LEGISLATIVE LIAISON
85-3537

David,

Here is DoJ's statement on S. 1667 - I'll probably write up a note on the hearing & can send it if you're interested.

Patty

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

WITNESS LIST

HEARING ON
S. 1667
ELECTRONIC COMMUNICATION PRIVACY

BEFORE THE
SUBCOMMITTEE ON PATENTS, COPYRIGHTS AND TRADEMARKS

November 13, 1985
9:30 a.m.
ROOM SD-226 DIRKSEN SENATE OFFICE BUILDING

I. The Honorable Robert W. Kastenmeier
Chairman
Subcommittee on Courts, Civil Liberties
and the Administration of Justice
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C.

The Honorable Carlos J. Moorhead
U.S. House of Representatives
Washington, D.C.

II. James Knapp, Esq.
Deputy Assistant Attorney General
Criminal Division
Department of Justice
Washington, D.C.

III. Mr. Philip M. Walker
Vice Chairman
Electronic Mail Association
Washington, D.C.

Michael Nugent, Esq.
Chairman, Privacy Committee
Association of Data Processing
Service Organizations
Arlington, Virginia

Mr. John Stanton
Chairman
Telocator Network of America
Washington, D.C.

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

IV. Dr. Lynn Ellis
Chairman, Committee on Communications
and Information Policy
Institute of Electrical and Electronic
Engineers
Washington, D.C.

accompanied by: Dr. P. Howard Patrick
Institute of Electrical
and Electronic
Engineers

Jerry Berman, Esq.
Chief Legislative Counsel
American Civil Liberties Union
Washington, D.C.

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Department of Justice

STATEMENT

OF

JAMES KNAPP
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE

THE

SUBCOMMITTEE ON PATENTS, COPYRIGHTS AND TRADEMARKS
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

S. 1667, ELECTRONIC COMMUNICATIONS PRIVACY ACT

ON

NOVEMBER 13, 1985

ILLEGIB

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1985

Mr. Chairman and Members of the Subcommittee, I appreciate the opportunity to appear here today to discuss S.1667, the Electronic Communications Privacy Act of 1985.

The proposed legislation is directed primarily at amending Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to provide coverage of new technologies in the area of communications and electronic surveillance that were not available when the original act was passed in 1968. In addition, the proposed legislation provides for more comprehensive judicial supervision of investigative methods related to electronic surveillance heretofore not within the scope of Title III.

We have serious concerns about many of those provisions of this bill which could unnecessarily complicate procedures without enhancing individual rights of privacy.

An in depth review of the proposed legislation is presently being conducted by several Department of Justice components whose

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

activities would be affected by this bill. Because of the complexity of this type of legislation that analysis has not yet been completed. The President's Commission on Organized Crime is also in the process of evaluating the effectiveness of Title III and it is my understanding that the Commission will be making recommendations relative to the effectiveness of the statute in the near future. So rather than addressing the specific language of the bill, I will limit myself to making a number of general comments and observations about certain proposals in the legislation, and then identifying some particular problems which we feel ought to be addressed.

Initially, I would note that Title III electronic surveillance is an extremely valuable and effective law enforcement tool. Its value was proved recently by a survey taken by the Criminal Division's Office of Enforcement Operations to test the results of court ordered electronic surveillance in 1983. That year was chosen to give sufficient time for investigations to be completed and most trials to be over. We chose, at random, 51 investigations which, with related wiretap authorizations, covered 35% of the total of new Title III authorizations for that year. All reports are still not complete, but our figures indicate that convictions, indictments and ongoing investigations in which indictments are expected have

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

occurred in 45 of the 51 investigations; which is a rate of 88%. In addition, in just 38 completed investigations, convictions of those originally named as interceptees or others later found to have been involved in the investigation total 467 or an average of almost 13 convictions per completed investigation. Currently another 64 individuals are under indictment in the remainder of the open investigations and a good number of further indictments are expected in those investigations that still have not reached the indictment stage.

We believe these figures, which we continue to amass and analyze, show the great effectiveness of Title III as a law enforcement tool. We must also stress that there is no record of abuse of electronic surveillance and that the rate of suppression of evidence obtained by means of electronic surveillance for any reason is minuscule.

As you know, the current laws governing interception of communications are complex and attempt to strike a balance between legitimate privacy concerns and the responsibility of federal officials to arrest and prosecute criminals. While we in the Department of Justice are mindful of the privacy rights of our citizens, we think it is equally necessary to recognize the importance of court-ordered interceptions of communications in

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

investigating major crimes. In the Department's judgment, Title III of the Omnibus Crime Control and Safe Streets Act has succeeded in providing an appropriate balance between the citizen's right to privacy and the law enforcement and societal interest in preventing crime and apprehending criminals. The statute has proven itself amenable to application to a number of new technologies although certainly not to all that have been developed. In addition, since the enactment of the statute in 1968, a substantial body of case law has developed which establishes well defined limits on how the statute is to be used and how it is to be interpreted. Relative to any assessment of the statute in terms of proposed amendments to address technological developments, care must be taken not to impair this existing and by now well understood statutory structure.

Moreover, before bringing certain investigative aids under judicial supervision, as the proposed bill does, great care must be taken to balance new impediments to important and well established investigative techniques against the degree of intrusion involved. In our view, judicial supervision is required when the degree of intrusion is such that it infringes upon an individual's reasonable expectation of privacy. This, of course, is the principle embodied in Title III and in the Supreme Court's decisions interpreting the Fourth Amendment.

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

I. NEW TECHNOLOGIES

The Department of Justice does agree that the electronic surveillance provisions of Title III should be re-evaluated periodically to ensure that the statute keeps pace with developing technology. Our policy is to propose amendments to the statute and to support those amendments proposed in Congress whenever our experience and continuing review of the statute warrant such action. At the present time, we recognize that certain modifications due to the rapidly changing technology of electronic communication may be necessary and we feel that some of the amendments proposed in S.1667 address this need. We would stress, however, that a great deal of further analysis and discussion is required before the implications of the new technology are fully understood.

ILLEGIB

ILLEGIB

DIGITAL TRANSMISSIONS

A. CELLULAR AND CORDLESS TELEPHONES

Although the Department believes that all forms of conventional telephones as well as many of the newer technologies are currently covered by Title III because the transmission is at

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

least in part by wire, there may be a need to amend the statute to specifically cover those types of telephones, like cellular telephones and certain forms of cordless telephones, where the communication is transmitted partly by means of radio. The radio portion of the transmission is either analog (regular voice transmission), digitized, or encrypted in some other fashion. The analog transmission would readily be subject to interception by an ordinary citizen with a standard AM/FM radio receiver by tuning to certain frequencies. Digitized or otherwise encrypted transmissions would require specialized equipment to turn the conversation back into analog form. In amending the statute to cover these new forms of telephones, a decision has to be made as to whether all communications should be covered including analog conversations when transmitted as radio communications. If so, would an ordinary citizen who intercepts them be subject to criminal or civil liability? Should there be a reasonable expectation of privacy where such calls are so suspectible to interception? In the alternative, should amendments to the statute respecting these types of telephones only be extended to the radio portions of the communications that are digitized or encrypted in some other manner where additional technical steps must be taken to turn the digitized communication back into analog form so it could be understood?

The Department has not yet formulated a policy on whether only a digitized or otherwise encrypted conversation should be

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

subject to the protection of the statute. It could be argued that the additional protection for the call by digitizing or otherwise encrypting it would evince a clear intent that there is a reasonable expectation of privacy. In this scenario, the citizen who either voluntarily or involuntarily intercepts the analog call would be free of criminal or civil liability. Obviously, so too should law enforcement personnel. These are questions that have to be looked at carefully before definitive recommendations can be made.

B. COMPUTER TRANSMISSIONS AND ELECTRONIC MAIL

Second, with respect to the legislation's attempt to bring within the proscriptions of Title III the newer types of non-aural transmissions such as computer transmissions and electronic mail, it is our current belief that with respect to authorization for the government to seize the contents of these transmissions, they are covered by an ordinary search warrant process based on probable cause pursuant to Rule 41 of the Federal Rules of Criminal Procedure. For example, if the government presently wishes to intercept a letter posted with the Postal Service, a search warrant under Rule 41 is procured. The Department believes that electronic mail is entitled to no greater protection than regular mail. Including these transmissions in

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Title III would, in effect, be adding an entire new scope to the existing statute. Had Congress intended that in 1968, it would have added non-aural communications such as ordinary mail in the statute at that time. The Department feels that changing the entire thrust of Title III is not warranted at this time and that intercepting this type of non-aural communication by private individuals could better be handled by separate legislation. The safeguards regulating government interception at this time are adequately covered by Rule 41 of the Federal Rules of Criminal Procedure. A similar analysis appears appropriate for computer transmissions.

ILLEGIB

C. VIDEO SURVEILLANCE

Video surveillance is a relatively new investigative tool. Two different types of situations must be considered when trying to legislate controls over this technology. The first is the situation where the government is conducting video surveillance of an individual or a premises where there is a reasonable expectation of privacy. The second type of video surveillance is where a closed circuit video transmission is intercepted by either the government or an individual.

The most common type of situation that arises with respect to government activity is the surveillance of an individual or a

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

premises where there is a reasonable expectation of privacy. Under present case law, the government would secure an order in the nature of a search warrant under Rule 41 of the Federal Rules of Criminal Procedure where there is only video surveillance, assuming the video surveillance involves a reasonable expectation of privacy. If there is to be any audio interception then a separate Title III authorization is procured. Under this procedure the rights of the citizen are adequately safeguarded. Adding video surveillance by itself to Title III would again be adding an entire new scope to the statute. The Department sees no need for that at this time particularly since most instances of video surveillance do not involve areas where there is a reasonable expectation of privacy. We would have no objection to authorizing courts to approve a continued video and audio surveillance in a single Title III order.

Considering the scenario where a closed circuit television transmission between two individuals would be intercepted, it is highly unlikely that such a transmission would take place without an audio portion relaying information on the image. Where the audio transmission is present, Title III adequately covers the communication. Interception of the video portion alone by government agents would be covered by Rule 41 so the only difficulty arises where the video transmission (with no audio

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

accompanist) is intercepted by someone other than a law enforcement officer. This very rare situation could be covered in the same type of legislation that would regulate computer hacking without disturbing the purpose and intent of Title III.

II. INVESTIGATIVE TECHNIQUES

With respect to S.1667, the Department has serious objections to several of the bill's other provisions in the areas involving those investigative techniques somewhat related to Title III but not presently within the coverage of that statute. The thrust of these provisions is to take investigative techniques that do not approach the level of intrusion involved in the actual interception of the contents of communications accomplished by full scale electronic surveillance and elevate them virtually to the same level. The result will be a severe hindrance to law enforcement in using non-intrusive techniques to combat drug trafficking, organized crime, and terrorism.

A. PAGING DEVICES

Although not specifically delineated in the proposed legislation, the new definitions would include paging devices under the proscriptions of the revised Title III.

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

There are presently three types of such devices. The first type, the tone pager, only transmits a beeping sound to the handset carried by the subscriber. No message of any type is transmitted and it is the Department's position that interception of the beep does not constitute a search and should not be regulated under the statute. The second type, the digital beeper, transmits digitized numbers and arguably a "message" could be transmitted by using numbers. Present practice is to procure an order under Rule 41 of the Federal Rules of Criminal Procedure based on probable cause to intercept this type of communication. Since no aural message is transmitted, it is the Department's position that Title III does not presently apply to this type of paging device. The third type of paging device, the voice pager, does in fact transmit an aural message and present practice is to secure an interception order under Title III before this type of message is intercepted.

It is the Department's position that present standards balance the rights of the individual with the interests of law enforcement and that new legislation should not escalate the levels of judicial supervision for the utilization of these devices over present standards. The third type of paging device should appropriately remain under Title III, while the second

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

type should continue to be regulated by Rule 41 of the Federal Rules of Criminal Procedure. The first type which transmits a beep only should not be subject to judicial supervision because of the de minimus level of intrusion.

The Department has no objection to codifying existing standards but would object to increased levels of supervision as imposing an undue burden on the use of the devices by law enforcement agents.

B. PEN REGISTERS

S.1667 would amend Title 18 of the United States Code to add a new chapter bringing the use of pen registers and location detection devices (tracking devices) under increased judicial supervision. It is the Department's position that this change would create serious problems in the law enforcement procedures that have developed under Title III.

Pen registers are attached to telephones only for the purpose of identifying and recording dialed numbers. Their use does not infringe on any constitutionally protected interest and that has clearly and definitively been decided by the Supreme Court. Smith v. Maryland, 442 U.S. 735 (1979). Pen registers

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

have proven to be a valuable tool in criminal investigations, especially those involving drug trafficking, organized crime activities, and money laundering where perpetrators frequently use the telephone to communicate. The pen register enables the investigators to establish a pattern of communication between suspects. It never permits access to the contents of a conversation. It is currently the practice of the Department to secure court orders authorizing the use of pen registers pursuant to Rule 57 of the Federal Rules of Criminal Procedure. Assistant United States Attorneys in the field may secure these orders, without the review of senior Department officials, upon a representation to the court that such information is relevant to an ongoing criminal investigation. Inasmuch as this procedure does not require a showing of "probable cause" to obtain the order, pen registers have proven especially effective at the earlier stages of investigations when the primary objectives are identifying the participants and determining their relationship in the alleged criminal activity. In many instances, the results of the pen registers are then used to develop the more detailed showing of "probable cause" necessary to obtain Title III orders authorizing the far more intrusive interception of wire and oral communications.

The proposed bill at page 16 establishes a standard of reasonable cause to believe that the information likely to be

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

obtained by such installation and use is relevant to a legitimate criminal investigation before a pen register can be authorized. The Department objects to this language. It escalates the level of judicial review in a manner inappropriate to the degree of intrusion on privacy interests that pen registers cause. If the assistant United States Attorney makes a representation to the court that a pen register is relevant to a criminal investigation, that should be sufficient and more should not be required. The difference between "reasonable" and "probable" cause is not readily discernible and this ambiguity would, we think, result in too great a degree of proof.

Bringing the use of pen registers within increased judicial supervision would limit their use and would impose many of Title III's elaborate procedures. Consequently, the use of pen registers would significantly decline to the detriment of criminal investigations and ultimately the prosecutions themselves. Given that pen registers, by comparison to the interception of communications, constitute a minimal intrusion into the privacy interests of targeted subjects, it is the Department's view that it is unnecessary and inappropriate to increase judicial supervision over their use.

Given that no communications are intercepted and that the courts have held that there is no constitutional or statutory requirement for court supervision of a pen register, the bill's

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

elaborate notification and reporting requirements would create an unnecessary burden on law enforcement resources that would not be balanced by an equal benefit to citizen rights of privacy.

C. LOCATION DETECTION DEVICES (TRACKING DEVICES)

Similarly, to include location detection devices (tracking devices) under Title III would have an adverse impact on law enforcement efforts. In most instances the use of location detection devices (tracking devices) like pen registers, invades no constitutionally protected interests. See e.g., United States v. Knotts, 460 U.S. 276 (1983). Such devices never reveal the content of any conversation. In those cases in which the installation or monitoring of location detection devices (tracking devices) would invade a subject's reasonable expectation of privacy, e.g., United States v. Karo, 104 S. Ct. 3296 (1984), court orders pursuant to a showing of "probable cause" are sought under Rule 41 of the Federal Rules of Criminal Procedure. In these instances as well, however, review and approval of the applications by senior Department officials is not required.

Like pen registers, location detection devices (tracking devices) have proven to be an effective and often vital investigative tool, especially in drug investigations where they

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

are used to track shipments of contraband and vehicles that transport those shipments. Their use often eliminates the need to commit substantial resources required for "moving" physical surveillance. The practical effect of subjecting the use of location detection devices (tracking devices) to increased judicial and administrative supervision would be to narrow severely the circumstances in which they could be effectively utilized. Because location detection devices (tracking devices) like pen registers very rarely involve any infringement into the privacy interests of the subject, it is unnecessary to impose upon their use the stringent controls and reporting requirements.

In addition, the reporting requirements imposed by the legislation would cause serious difficulties in the utilization of these procedures. The Department feels that the minimal levels of intrusion involved in using these devices does not warrant significant reporting requirements.

D. TOLL RECORDS

The proposed bill has a provision that would add to Title 18 a new subsection 2511(4), which would require a court order for the government to obtain telephone toll records. Telephone toll records, like pen registers, never reveal the contents of a conversation and invade no reasonable expectation of privacy.

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Even if the criteria required for securing the order under the bill -- reasonable suspicion that a person or entity by whom or to whom the communications were made has engaged, or is about to engage, in criminal conduct and that the records may contain information relevant to the conduct -- does not rise to the probable cause level required for securing an eavesdropping court order, the requirement nevertheless does impose a heavy procedural burden on law enforcement officials in an area that is minimally intrusive and has proven to be a highly effective law enforcement tool. It is the view of the Department of Justice that present procedures for securing this information by either an administrative subpoena from a law enforcement agency with such power or by way of a grand jury subpoena provide sufficient safeguards against the abuse of this process.

F. ADDITIONAL PROCEDURAL REQUIREMENTS

The additional requirements imposed by the proposed legislation relative to providing further specific information in the applications and the orders on a) investigative objectives and b) alternate investigative techniques are unnecessary and would be more burdensome. The statute and the case law that has developed clearly defines the parameters of what is necessary to obtain the order. The law is clear that electronic surveillance

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

need not be the only remaining alternative as long as the court is satisfied that the other investigative methods are likely not to succeed or would be too dangerous. That showing must now be made before an order is issued.

The Department would oppose the proposed amendment to 18 U.S.C. 2518 (8)(a) that would change the wording of that portion of the statute which mandates presenting the recording tapes of the intercepted conversations to the judge "immediately" upon the expiration of the authorization to presenting the tape recordings "not later than 48 hours", courts have clearly held that they should be presented as soon as possible but that, for good cause shown, courts can excuse delays depending upon the situation. Current case law has given this discretion to the judge and legislating a specific time would be too limiting in practice and would require re-interpretation by the courts. Nor is there any practical reason to mandate ten day reviews by courts of the status of individual wiretaps. Courts are presently able to impose such requirements, where warranted at appropriate intervals.

Finally, we wish to draw attention to the changes in the proposed level of culpability of a violator in both the criminal and civil areas. Section 2520 of Title 18 currently provides that a good faith reliance on a court order or legislative

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

authorization is a complete defense to both civil and criminal actions brought under Title III or any other law. Section 103 of the proposed legislation, which is intended to replace Section 2520 of the current statute, provides that a good faith reliance on a court order or warrant is a complete defense to only a civil action. Thus, the implications of the proposed legislation are unclear as to the level of criminal liability of an agent who in the course of his or her duties inadvertently violates the law. To impose a criminal liability for what would at most be ordinary negligence is exceedingly harsh and would inhibit those involved in conducting legitimate investigations. The Department would like to see a good faith exception to both criminal and civil liability as well as a good faith exception to the exclusionary rule for presentation of evidence under appropriate circumstances.

III. AFFIRMATIVE RECOMMENDATIONS

The Department in its experience with the provisions of Title III has identified certain areas where affirmative amendments would greatly facilitate the law enforcement function.

The first of these areas is the extension of Title III authorization authority to interceptions of specified individuals wherever they may be as well as to places and facilities in line

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

with the theory of Katz v. U.S. 389 U.S. 347, that the Fourth Amendment protects people not places. We realize this suggestion raises interesting and novel issues of a constitutional nature. We raise it to stimulate debate at this time in the hope that an appropriate vehicle can be drafted to permit this form of authorization.

We also recommend extending Title III authorization to cases involving bail jumping where the underlying offenses would have supported a Title III request and to prison escapes. We support the addition of the new offenses in Section 105 of the proposed legislation and would recommend adding air piracy and hostage taking to those offenses.

The Department favors the proposed provision of the bill that would authorize an Acting Assistant Attorney General in charge of the Criminal Division to sign Title III authorizations.

The Department endorses the proposed legislation's provisions that would authorize the use of mobile interception devices (p. 11 of the statute) and tracking devices (p. 16 of the statute) across district lines where the order is procured in the district of origin.

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8

An amended statute should have a provision that the 30-day authorization period for a Title III should begin to run upon installation of the interception device and not on signing of the order.

The Department also favors expanding the category of people who can help monitor the interception of communications, such as clerical personnel in the enforcement agencies.

In conclusion, new technologies may warrant a re-examination of the scope and adequacy of existing Title III provisions now available. We feel that some additional study and review should be considered. Consideration should also be given to the changes that the Department has suggested. These changes listed are not exhaustive of those changes that might facilitate effective and proper use of Title III, but they are illustrative of practical problems which could be solved by new legislation. We would be pleased to work with the Subcommittee's staff in developing a bill that all can support.

Mr. Chairman, that concludes my prepared remarks and I would be happy to answer any questions at this time.

Sanitized Copy Approved for Release 2010/04/21 : CIA-RDP87M01152R001101390004-8